REMARKS

A. INTRODUCTION

The Final Office Action has been received and carefully considered. Claims 1-25 are pending in the application. In this response, no amendment has been made to the claims or other parts of the application. Applicant still believes that the application is in condition for allowance and notice thereof is respectfully requested.

Applicant maintains the traversal of the obviousness rejection and will respond to the Examiner's arguments in Section C.

B. THE REJECTION UNDER 35 U.S.C. § 103

In page 2 of the Final Office Action, claims 1-2, 11-13 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Sit *et al.* (US Patent 6,349,336, hereinafter "Sit") in view of Epstein *et al.* (US Patent 6,584,508, hereinafter "Epstein"). In page 4 of the Final Office Action, claims 3-4 and 14-15 are rejected under 35 U.S.C. §103(a) as being unpatentable over Sit, Epstein and further in view of Fan *et al.* (US Patent 6,219,706, hereinafter "Fan"). In page 5 of the Final Office Action, claims 5-10 and 16-24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Sit, Epstein, Fan and further in view of Albert *et al.* (US Patent 6,687,222, hereinafter "Albert").

These rejections are improper for at least the following reasons. (1) The combinations of Sit with the other references fail to teach or suggest all the elements in the claimed invention. (2) There is no suggestion or motivation in the cited references or in the general knowledge to make the combinations.

Applicant's invention, as recited in independent claims 1 and 12, is directed to a secured file transfer protocol (FTP) system and method. Embodiments of the present invention

specifically address the difficulties faced by a FTP client behind a firewall. In one embodiment, two FTP proxy systems (e.g., a FTP client proxy system 12 and a FTP server agent 14 in Figure 2) are positioned astride a firewall device. The client-side FTP proxy system (e.g., the FTP client proxy system 12) has a FTP-like session with the FTP client. The server-side FTP proxy system (e.g., the FTP server agent 14) has a FTP-like session with the FTP server. The two FTP proxy systems communicate with each other securely across the firewall device via a single port thereon. One advantage of such an embodiment is to prevent the firewall from opening and closing random ports as in traditional FTP sessions.

Sit discloses a hypertext transfer protocol (HTTP) tunneling action that allows a remote processor to communicate with a local processor when the remote processor is coupled to the local processor via a reverse proxy device, a computer network, a firewall and a proxy agent device. The primary goal in Sit is to trick the firewall into believing that an incoming request is actually a response to an outgoing request, so that the remote processor may access/control the local processor behind the firewall. *See* Sit: col. 2, lines 39-60 and col. 3, lines 36-48.

Epstein discloses an advanced data guard having independently wrapped components. One of the independently wrapped components may be a FTP proxy. *See* Epstein: Figure 4.

Applicant's following arguments regarding the primary references Sit and Epstein will moot the obviousness rejections further based on Fan and Albert.

(1) The Sit-Epstein Combination Fails to Teach or Suggest All the Elements in the Claimed Invention.

As stated in MPEP § 2143.03, to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (C.C.P.A. 1974). That is, "[a]ll words in a claim must be considered in

judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 165 USPQ 494, 496 (C.C.P.A. 1970).

Individually or in combination, Sit and Epstein do not teach or suggest (i) "*restricting [FTP] data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall*" or (ii) "*restricting all flow of FTP data passing through said security system through a single port on said firewall.*" Claim 12. *See also*, Claim 1.

A search of the Sit reference reveals that Sit never uses the terms "port" or "FTP" or "file transfer protocol." Though Epstein mentions "ports" or "TCP/IP ports" several times, none of those are in the context of FTP. Nor does Epstein provide any teaching or suggestion of restricting data flow to a single port in a firewall.

In the Office Action, the Examiner asserts that the following sentence in Sit teaches "said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall" as recited in claim 1:

> "Firewall 305 protects devices on the internal side 302 from unwanted communications originating with devices on the external side 304.." Sit, col. 7, lines 26-28.

However, apart from the reference to a firewall, the above-quoted sentence has no relevance to the limitation of restricting data flow to a single firewall port. If the Examiner meant that the generic protective function of the firewall 305 includes restricting data flow to a single port, such a broad reading of the Sit reference is improper.

Even if the presence of the firewall 305 did imply that the proxies on either side use a single firewall port to communicate, it still has no relevance to FTP sessions through a firewall as addressed in the claimed invention. When servicing a HTTP session, the two proxies may be

in "persistent connection" with each other and might use a single firewall port. A "persistent connection" between an HTTP client and an HTTP server is mandated by HTTP/1.1 standard, which specifies that "HTTP implementations SHOULD implement persistent connections." Fielding, et al., Hypertext Transfer Protocol -- HTTP/1.1, Network Working Group RFC-2616, June 1999, page 43. Thus, there is nothing remarkable about a persistent HTTP connection between the two proxy systems, as the single connection is the norm for an HTTP session, whether or not it is through a firewall.

For an FTP session, on the other hand, this is not the case. In many ways, an FTP session through a firewall is completely different from an HTTP session through a firewall. First, a typical FTP session needs at least two TCP connections, one control connection and one data connection. Postel et al, FILE TRANSFER PROTOCOL (FTP), Network Working Group STD-9 (RFC-959), October 1985, pages 3 and 7. In the present application, the control connection is referred to as a "command channel," and the data connection is referred to a "data channel." Second, although "[t]he FTP specification says that by default, all data transfers should be over a single connection, ... most current FTP clients do not behave that way." Instead, "[a] new connection is used for each transfer; to avoid running afoul of TCP's TIMEWAIT state, the client picks a new port number each time and sends a PORT command announcing that to the server." Alternatively, "if the client sends a PASV command, the server will do a passive TCP open on some random port, and inform the client of the port number. The client can then do an active open to establish the connection." Bellovin, Firewall-Friendly FTP, Network Working Group RFC-1579, February 1994, page 1. Therefore, in practice, more than two connections are typically used for one FTP session. Third, because of the multiple-connection requirement, an FTP session through a firewall often requires the opening and closing of multiple random ports

in the firewall to accommodate the data connection. That is, a firewall port randomly assigned for one FTP data connection does not remain open indefinitely. "After requested data are sent to the passive FTP client system 2 by the FTP server 4 over the data channel, the FTP server 4 and the firewall 10 dynamically close the corresponding logical communication ports until the next data channel transmission." Page 9, lines 5-9.

Further, the above-quoted sentence does not say anything about restricting all data flow to a single port in the firewall. While one connection is kept open between the two proxy devices for one HTTP session, there is no suggestion that the same connection or the same port will be used for all HTTP sessions (i.e., all data flows) between the two proxy devices. As such, multiple random ports (or TCP sockets) may still be opened and closed in the firewall for multiple HTTP sessions. In the present invention, however, "a single outbound connection between the FTP client proxy system 12 and the FTP server agent 14 uses a single port on the firewall 10 and multiplexes a plurality of FTP sessions between a plurality of FTP servers 4 and a plurality of passive FTP client systems 2." Page 19, lines 2-5 (emphasis added). *See also*, Figures 3 and 4.

For at least these reasons, there is no basis to equate a persistent HTTP connection with a single-port FTP through a firewall. Since neither Sit nor Epstein teaches or suggests "*restricting all flow of FTP data passing through said security system through a single port on said firewall*," their combination cannot render the claimed invention obvious.

(2) There Is No Suggestion or Motivation to Combine or Modify Sit and Epstein.

As stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the

knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

Since no such "teaching, suggestion, or motivation" can be found in the cited references or in general knowledge, the obviousness rejection of the pending claims is improper.

The text of Sit does not provide any explicit suggestion or motivation to combine with Epstein. Sit makes no reference whatsoever to the terms "FTP" or "file transfer protocol." Therefore, Sit provides no explicit motivation to modify its system for FTP sessions.

Neither is there any implicit suggestion for the modification. First, Sit focuses exclusively on HTTP sessions, which, as described above, are completely different from typical FTP sessions in terms of the required number of connections and firewall ports. It is hardly obvious how such a HTTP-specific implementation could be adapted for FTP traffic. Second, Sit's primary goal is to allow an outside computer to access and control a local computer behind a firewall. To achieve this goal, Sit implements two HTTP proxies to trick the firewall into believing the incoming requests are responses to some outgoing requests. This trickery on the firewall achieves exactly what a secured FTP architecture tries to avoid. In the present invention, the security of the firewall is not in anyway circumvented or compromised. Claim 1 recites "said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall." Thus, the firewall in the present invention still functions as it is designed to. All FTP data between a local FTP client and an external FTP server are multiplexed onto a single-port secured connection between the two proxy systems. It is difficult to imagine that a network engineer mindful of firewall security would be inspired by Sit's security-bypass measures to build a secured FTP system as claimed.

Nor does Epstein provide any suggestion or motivation to combine with Sit. Epstein uses an internal content-based filter to enhance security of a multi-part proxy based firewall or guard. A single FTP proxy is included in the multi-part proxy. *See* Epstein: Figures 2 and 4. Such traditional single-proxy FTP application is not amenable to adaptation in the two-HTTP-proxy environment as disclosed in Sit.

The Examiner cites the following passage to suggest that Epstein is readily combinable with Sit:

> "Proxy server 200 generally includes an operating system 204 (possibly hardened) operating on computing hardware 202. Proxy server 200 also includes a plurality of proxy applications, shown in FIG. 2, including, for example, HTTP proxy application 206A, SMTP proxy application 206B, and FTP proxy application 206C." Epstein: col. 4, lines 16-20.

However, apart from briefly mentioning "HTTP proxy application" and "FTP proxy application" in the same sentence, this passage has no relevance to the Sit reference. In fact, in this passage and in six other instances where the term "FTP" is used (i.e., Epstein: col. 1, line 37; col. 2, line 27; col. 4, lines 4-5 and 10), Epstein only refers to well-known standard FTP operations and regular FTP proxies. Other than listing FTP proxy application as one possible component in a multi-part proxy, Epstein says nothing that is even remotely related to Sit's two-HTTP-proxy setup or the present invention's two-FTP-proxy architecture.

Since neither Sit nor Epstein provides any motivation to combine, in order for the obviousness rejection to stand, such motivation must come from the knowledge generally available to one of ordinary skill in the art. However, that is not the case here. In order to solve the problems uniquely associated with FTP sessions through a firewall, an artisan must first identify such problems. As recognized in the present application, the specific problems include, for example, the "potential security exposures" caused by "dynamic opening and closing of ports

on a firewall," and the "significant administrative resources" "required to configure a firewall to allow communication over a large range of sources and destinations." Page 9, lines 17-21. The recognition of such problems is an essential part of the present invention, which leads to a secured FTP architecture as claimed. Yet, there is no indication in the cited references that these problems were ever recognized or identified prior to the time of the present invention. Nor are these problems easily recognizable by a person of ordinary skill in the art.

Further, the HTTP-based Sit system cannot be mechanically combined with Epstein for implementation of a secured FTP system as claimed. Even if Sit and Epstein were combinable, the combination does not disclose each and every element in the claimed invention. Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Without a clear recognition of the problems associated with FTP sessions through a firewall, the desirability of the combination is not apparent from the cited references.

Since the requisite suggestion or motivation is not found in the references themselves or in the knowledge generally available, the Final Office Action has failed to establish a *prima facie* case of obviousness. Withdrawn of the obviousness rejection is respectfully solicited.

C. RESPONSE TO THE EXAMINER'S ARGUMENTS

In the "Response to Arguments" section of the Final Office Action, the Examiner cited various portions of Sit and Epstein in an attempt to reject Applicant's arguments presented in a previous response. Applicant respectfully submits that the Examiner's reliance on the cited references is misplaced.

(1) The Sit System is Limited to HTTP.

In page 8 of the Final Office Action, the Examiner asserts that "the [Sit] invention can be applied to HTTP and other message transfer protocols such as Simple Mail Transfer Protocol (SMTP)." In support, the Examiner cites "Field of the Invention" section (col. 1, lines 9-10) as well as the following passage from Sit:

> "CDMG 125 will also initiate communication in response to a communication initiation command 140 received via electronic mail (email). Using Simple Mail Transfer Protocol (SMTP), remote processor 157 can send a communication initiation request 165, which is stored on email server 135 as communication initiation request 165a." Sit: col. 4, lines 45-50.

Because the "Field of the Invention" makes a general statement that Sit "relates to message transfer across a firewall," and because the above-quoted passage briefly refers to SMTP, the Examiner comes to the conclusion that Sit is adaptable for other message transfer protocols such as FTP. Applicant cannot agree.

It is well known that the "Field of the Invention" section in a patent document only states the general field of the claimed invention in that document. The "Field of the Invention" statement almost always encompasses a much broader scope than what is actually disclosed in the patent document. Therefore, it is improper to rely on that section as evidence of what the patent document specifically discloses. According to the "Field of the Invention" in Sit, it is only clear that Sit relates to some type of message transfer across a firewall. As to specific message transfer protocols, the "Field of the Invention" says or proves nothing.

As to the brief reference to SMTP protocol, a close examination of Figure 2 in Sit will reveal that SMTP is hardly relevant to the proxy system at all. The SMTP protocol is mentioned only because the remote processor 157 emails a communication initiation request 165 which is subsequently stored on the email server 135. The transmission and storage of an email communication involves the SMTP protocol because it happens to be the *de facto* standard for

email transmission over the Internet. Otherwise, the SMTP protocol has nothing to do with the proxy system disclosed in Sit. For example, in Figure 2, the email server 135 is connected in such a way that it is not affected by the proxy machine 145 at all. Other than this instance, Sit does not refer to SMTP anywhere else. Everywhere else, Sit refers to its reverse tunneling protocol as, for example, "reverse HTTP communication protocol" (col. 7, line 5) or "reverse http [sic] protocol" (col. 7, lines 11-12). In the first paragraph of its "Detailed Description" (col. 3, lines 36-49), Sit defines the terms "request" and "response" strictly in the context of HTTP protocol. Throughout, the Detailed Description speaks of "Web browsers" and "Web sites" and never deviates from HTTP message transfers. Even in the last paragraph of the Detailed Description (col. 8, lines 35-52), where alternatives and modifications are discussed, there is not a slightest hint that any protocols other than HTTP could be implemented with the disclosed proxy system.

In view of the foregoing reasons, any person of ordinary skill in the art would recognize that Sit is limited to HTTP only.

(2) Neither Sit Nor Epstein Discloses Multiplexing Capability Between Two Proxies.

In page 8 of the Final Office Action, the Examiner asserts, without elaboration, that "Figure 5 of Sit et al. indicates the multiplexing capability of reverse proxy 312 and the proxy agent 306." The Examiner appears to reach this conclusion solely based on the illustration of two links (one numbered 301, the other un-numbered) among the reverse proxy 312, the firewall 305 and the proxy agent 306. Otherwise, the term "multiplex" or its variations do not appear anywhere in the Sit reference. However, if the Examiner infers the multiplexing capability simply because the links are shown as single lines, the Examiner is probably mistaken. The links may actually represent multiple lines or parallel cables. For example, at least the link 301,

referred to as "a computer network 301 such as the Internet," is not a single-line connection. Sit: col. 7, lines 24-25. It is unclear what kind of physical connection the un-numbered link, between the firewall 305 and the proxy agent 306, represents.

In page 9 of the Final Office Action, the Examiner further quotes the following passage to show that Epstein discloses either multiplexing capability or single-port HTTP connections through a firewall:

> "Fourth, the very essence of a proxy is network I/O. The proxy will therefore need to perform socket-related system calls. Depending on the proxy, it is possible to restrict the ports that the proxy is allowed to access so that the proxy cannot poke extra holes in the firewall. HTTP proxies will typically bind only to a default socket (e.g., 80). Accordingly, a software wrapper for an HTTP proxy can include a constraint such that the HTTP proxy can only bind to the default socket." Epstein: col. 6, lines 28-36 (emphasis added).

However, it should be noted that Epstein does not refer to "multiplexing" in this or any other passage. As to the single-port HTTP connections through the firewall, it should be noted that Epstein only suggested restricting "ports" (plural) rather than restricting "port" (singular). Further, it is well known that the default socket 80 that HTTP proxies bind to generally refers to ports in a web server rather than those in a firewall.

Even if, for argument's sake, the Examiner were correct in asserting that Epstein discloses using a single port in a firewall for HTTP sessions, it still would not render it obvious to use a single port for FTP sessions as presently claimed. The Examiner appears to place significant weight on the statement that "HTTP proxies will typically bind only to a default socket (e.g., 80)." It should be noted that the default use of port number 80 for HTTP comes from the Internet Assigned Numbers Authority (IANA) recommendations. The assignment of port number 80 to HTTP sessions is published by the IANA at the following website: http://www.iana.org/assignments/port-numbers. In the same publication, however, the IANA

also assigns, not one, but two port numbers to FTP sessions: port 20 for FTP data and port 21 for FTP control. Since the IANA recommendation is widely followed, the use of two ports for FTP sessions is a standard practice. Even if an artisan happens to contemplate a single firewall port for HTTP sessions simply by following the IANA recommendation of a single port (80), it is inconceivable that the artisan would at the same time ignore the other IANA recommendation of two ports for FTP session.

(3) There Is No Motivation to Combine Sit and Epstein.

In pages 9-10 of the Final Office Action, the Examiner attempts to refute Applicant's argument that there is no suggestion or motivation to combine or modify Sit and Epstein.

The Examiner starts by asserting again that Sit can be applied to HTTP and other message transfer protocols such as SMTP. As discussed above, the Examiner's understanding of Sit's reference to SMTP is erroneous and Sit contemplates no other protocol than HTTP.

The Examiner then, without explanation, points to Figure 5 in Sit and quotes the following passage:

> "The provision of reverse proxy 312 and agent 306 allows browsers 314I, 314E and Web servers 308I, 308E to be completely ignorant of the reverse tunneling procedure. The procedure is also transparent to applications such as 316I and 316E that interface directly with agent 306 and reverse proxy 312, respectively." Sit: col. 8, 22-27.

The Examiner further states that "Epstein et al. discloses a system wherein the proxy server includes a plurality of proxy applications, including FTP proxy application." A conclusion is then reached that "there is a motivation to combine the teaching of Epstein et al. with the system of Sit et al." Applicant fails to appreciate the relevance of the above-quoted passage. Nor can Applicant understand the Examiner's reasoning.

(4) New Intended Use Necessitates Structural Differences.

In page 10 of the Final Office Action, the Examiner asserts that "a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art." The Examiner further asserts that "if the prior art structure is capable of performing the intended use, then it meets the claimed limitations."

The Examiner's assertions, if correct, can only be applied to the system claims in the present application. If the Examiner recognizes that the pending method claims do recite new intended use of a "prior art" structure, then these method claims should be patentable. According to 35 U.S.C. § 101, "[w]hoever invents or discovers any new and useful process ... may obtain a patent therefor" (emphasis added). 35 U.S.C. § 100(b) further defines "process" as "process, art, or method, and includes a new use of a known process, machine, manufacture, composition of matter, or material" (emphasis added). So far, the Examiner has not produced any evidence that the claimed method for secured FTP through a single firewall port was ever disclosed in the prior art references. Therefore, the method claims 12-25 in the present application do recite a patentable new use.

As to the system claims 1-11, if the Examiner meant that the secured FTP systems recited therein bear no structural difference from the Sit system, the Examiner is mistaken. An implementation of a secured FTP system according to embodiments of the present invention necessarily involves the use of computing or communications hardware devices. Even if a physical arrangement of some of these hardware devices appears to be similar to that found in Sit, the inner workings or functions of these devices are quite different. For example, the server recited in claim 1 performs FTP-related functions while the servers in Sit are web servers. *See e.g.*, Sit: Figure 5, web servers 308E and 308I. The proxy servers in the present invention are FTP proxies while the proxy servers in Sit are HTTP proxies. Compare to Sit, the specific

functions of the firewall in the present invention are also different. For example, claim 1 recites the limitation of "said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall." Claim 1 also recites the limitation that "all FTP data are transferred between said client system and said server through said single port on said firewall." These limitations, not found in Sit or any other references, require that the hardware devices such as the server, the proxies and the firewall be programmed accordingly to provide the new secured FTP functions. Courts have consistently held that "programming [of a general purpose computer] creates a new machine, because a general purpose computer in effect becomes a special purpose computer once it is programmed to perform particular functions pursuant to instructions from program software. In re Alappat, 33 F.3d 1526, 1545 (Fed. Cir. 1994). *See also*, In re Freeman, 573 F.2d 1237, 1247 (C.C.P.A. 1978); In re Noll, 545 F.2d 141, 148 (C.C.P.A. 1976); In re Prater, 415 F.2d 1393, 1403 (C.C.P.A. 1969). It is undeniable that the Sit system, programmed and configured for HTTP connections, is incapable of accommodating FTP traffic. To adapt the Sit system to perform the secured FTP functions presently claimed, that is, if the Sit system is at all adaptable, substantial programming of a number of hardware devices is necessary. Therefore, the secured FTP systems as recited in claims 1-11 constitute new machines that are structurally different from the Sit system.

D. CONCLUSION

For at least the reasons provided above, Applicant respectfully submits that the application is in condition for allowance. Favorable reconsideration and allowance of the pending claims are respectfully solicited.

Should there be anything further required to place the application in better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number listed below before issuance of any further office action.

In the event any additional fees are due, the Commissioner is hereby authorized to charge the undersigned's Deposit Account No. 50-0206.

Respectfully submitted,

HUNTON & WILLIAMS, LLP

By: _____

Ce Li
Registration No. L0214

Hunton & Williams, LLP
1900 K Street, N.W., Suite 1200
Washington, D.C. 20006-1109
Telephone (202) 955-1500
Facsimile (202) 778-2201

Dated: 1/11/2006